COMPREHENSIVE WRITTEN INFORMATION SECURITY PROGRAM

I. Objective

Our objective in the development and implementation of this comprehensive written information security program ("WISP") is to create effective administrative, technical, and physical safeguards for the protection of personal information of Massachusetts' residents, and to comply with obligations under 201 CMR 17.00.

The WISP sets forth our procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of Massachusetts' residents. For purposes of this WISP, "personal information" means a Massachusetts' resident's first name (or initial) and last name, in combination with the resident's: (1) social security number; (2) driver's license number or state-issued ID card number; or (3) financial account number or credit/debit card number.

II. Purpose

The purpose of the WISP is to: (a) ensure the security and confidentiality of personal information; (b) protect against any anticipated threats or hazards to the security or integrity of such information; and (c) protect against unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. Scope

In formulating and implementing this WISP, we sought to: (1) identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information; (3) evaluate the sufficiency of existing policies, procedures, information systems, and other safeguards in place to control risks; (4) design and implement a WISP that puts safeguards in place to minimize risks, consistent with the requirements of 201 CMR 17.00; and (5) regularly monitor the effectiveness of those safeguards.

IV. Data Security Coordinator

We have designated Shari Blackman and Michael Hoffman to implement, supervise and maintain this WISP. Those designated employees (the "Data Security Coordinators") will be responsible for:

a. initial implementation of the WISP;
b. training employees;
c. regular testing of the WISP's safeguards;
d. evaluating the ability of each of our third-party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, consistent with 201 CMR 17.00;
e. requiring such third-party service providers by contract to implement and maintain appropriate security measures;
f. reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that may implicate the security or integrity of records containing personal information; and
g. conducting an annual training session for all owners, managers, employees, and independent contractors (including temporary and contract employees who have access to personal information on the elements of the WISP) and ensuring that all attendees certify their attendance at the training and their familiarity with the requirements for ensuring the protection of personal information.

V. External Risks

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information—and to evaluate and improve, where necessary, the effectiveness of the current safeguards for limiting such risks—the following measures will be effective immediately:

- There will be reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, installed on all systems processing personal information.
- There will be reasonably up-to-date versions of system security agent software, which will include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing personal information.
- To the extent technically feasible, all personal information stored on laptops (or other portable devices) and all records/files transmitted across public networks or wirelessly will be encrypted. Encryption here means the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by the Massachusetts Office of Consumer Affairs and Business Regulation.
- All computer systems will be monitored for unauthorized use of or access to personal information.
- There will be secure user authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning/selecting passwords or use of unique identifier technologies (e.g., biometrics or token devices); (3) control of data security passwords to ensure that such passwords are kept in a location.

VII. Internal Risks

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper, or other records containing personal information—and to evaluate and improve (where necessary) the effectiveness of the current safeguards for limiting such risks—the following measures are mandatory and effective immediately:

- A copy of the WISP will be distributed to each employee who will have access to personal information as outlined in the WISP, who must, upon receipt of the WISP, acknowledge in writing that he/she has received a copy of the WISP.
- There will be immediate retraining of employees on the detailed provisions of the WISP.
- Employment contracts will be amended immediately to require all employees to comply with the provisions of the WISP and to prohibit any nonconforming use of personal information during or after employment, with mandatory disciplinary action to be taken for violation of security provisions of the WISP. (The nature of the disciplinary measures may depend on a number of factors, including the nature of the violation and the nature of the personal information affected by the violation.)
- The amount of personal information collected will be limited to that amount reasonably necessary to accomplish our legitimate business purposes or necessary for us to comply with other state/federal regulations.
- Access to records containing personal information will be limited to those persons who are reasonably required to know such information in order to accomplish our legitimate business purposes or to enable us comply with other state or federal regulations.
- Electronic access to user identification after multiple unsuccessful attempts to gain access will be blocked.
- All security measures will be reviewed at least annually, or whenever there is a material change in our business practices that may reasonably implicate the security or integrity of records containing personal information. The Data Security Coordinator will be responsible for this review and will fully apprise management of the results of that review and any recommendations for improved security arising out of the review.
- Terminated employees must return all records containing personal information, in any form, that may be in their possession (including all such information stored on laptops or other portable devices or media, and in files, records, work papers, etc.).

- A terminated employee's physical and electronic access to personal information will be immediately blocked. He/she will be required to surrender all keys, IDs, access codes, badges, business cards, and the like, that permit access to the firm's premises or information. Moreover, such terminated employee's remote electronic access to personal information will be disabled; and his/her, e-mail access, internet access, and passwords will be invalidated. The Data Security Coordinators will ensure that the list of all lock combinations, passwords, and keys are secured by the Information System and Security Departments.
- Current employees' user ID's and passwords must be changed periodically.
- Access to personal information will be restricted to active users and active user accounts only.
- Employees are encouraged to report any suspicious or unauthorized use of customer information.
- Whenever there is an incident that requires notification under Mass. Gen. Laws ch. 93H, § 3, there will be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are required to improve the security of personal information for which we are responsible.
- At the end of the work day, all files and other records containing personal information must be secured in a manner that is consistent with the WISP's rules for protecting the security of personal information.
- Each department will develop rules (bearing in mind the business needs of that department) that ensure that reasonable restrictions upon physical access to records containing personal information are in place, including a written procedure that sets forth the manner in which physical access to such records in that department is to be restricted; and each department will store such records and data in locked facilities, secure storage areas, or locked containers. (See below for department-specific rules on physical access to records containing personal information.)
- Access to electronically stored personal information will be electronically limited to those employees having a unique log-in ID; and re-log-in will be required when a computer has been inactive for more than a few minutes.
- Paper or electronic records (including records stored on hard drives or other electronic media) containing personal information will be disposed of only in a manner that complies with Mass. Gen. Laws. ch. 93I. This means that (a) paper documents containing personal information will be redacted, burned, pulverized, or shredded so that personal data cannot practicably be read or reconstructed; and (b) electronic media and other non-paper media containing personal information will be destroyed or erased so that personal information cannot practicably be read or reconstructed.
- Any time that personal information is required to be transported off premises, it will be authorized by a Data Security Coordinator in advance and performed only by a WISP trained employee. The employee will remain in 100% visual contact with the information at all times and the information will be returned as soon as practical to the premises and secure it in a locked cabinet or office with restricted access.

VIII. Department Guidelines on Physical Access to Records Containing Personal Information

- **All Departments**
  - Personal applicant/employee information obtained through the internet will be printed and remain in 100% visual contact with the WISP trained employee until it can secured in a locked cabinet at Human Resources (no later than the close of business on the date the information is printed).

There are additional restrictions upon physical access to records containing personal information for the following departments:

- **Finance**
  - Each time that a physical record containing personal information is received, it will be maintained in a restricted area where the responsible, WISP trained party will have 100% visual contact with it to ensure no unauthorized persons gain access to the area or personal information.
  - At the end of the work day, all files and other records containing personal information will be secured in a locked cabinet or a locked office with restricted access.

- **Group Sales**
  - Each time that a physical record containing personal information is received, it will be maintained in a restricted area where the responsible, WISP trained party will have 100% visual contact with it to ensure no unauthorized persons gain access to the area or personal information.
  - At the end of the work day, all files and other records containing personal information will be secured in a locked cabinet or a locked office with restricted access.

- **Human Resources**
  - Each time that a physical record containing personal information is received, it will be maintained in a restricted area where the responsible, WISP trained party will have 100% visual contact with it to ensure no unauthorized persons gain access to the personal information.
  - At the end of the work day, all files and other records containing personal information will be secured in a locked cabinet or a locked office with restricted access.

- **Loss Prevention**
  - Each time that a physical record containing personal information is received, it will be maintained in a restricted area where the responsible, WISP trained party will have 100% visual contact with it to ensure no unauthorized persons gain access to the area or personal information.
  - At the end of the work day, all files and other records containing personal information will be secured in a locked cabinet or a locked office with restricted access.

- **Safety**
  - Each time that a physical record containing personal information is received, it will be maintained in a restricted area where the responsible, WISP trained party will have 100% visual contact with it to ensure no unauthorized persons gain access to the area or personal information.
  - At the end of the work day, all files and other records containing personal information will be secured in a locked cabinet or a locked office with restricted access.